**Amendments to the Specification**

**Page 1, lines 7-11 (Second Paragraph):**

This application also describes and claims subject matter that is in co-pending United States patent application filed simultaneously herewith and entitled: "METHOD AND APPARATUS FOR APPLICATION-INDEPENDENT END-TO-END SECURITY IN SHARED-LINK ACCESS NETWORKS," Serial No. 09/698,978.

**Page 6, line 18 through Page 8, line 6:**

Since the NAT does not have an ALG for an unsupported protocol, an ALG that would otherwise be implemented at the NAT is implemented instead at the client to perform any necessary functions on the packet payload and/or headers. The client having a client-implemented ALG is therefore enabled to communicate with a foreign address using a protocol that is not directly supported by NAT. In particular, a security protocol suite, such as IPSec, which is incompatible with NAT due to the inability of NAT to perform necessary modifications within the packet, can be used in order to ensure end-to-end security. Besides implementing the necessary ALGs, the client pre-compensates outgoing packets before they are transmitted and post-compensates incoming packets for the effects on the packets of the NAT's translations. The inclusion at the client of the necessary ALGs and pre and post compensation by the client is the subject of the afore-noted co-pending patent application Serial No. 09/698,978, filed on even date hereof. Specifically, for the IPSec protocol, each outgoing packet is modified by the client before being processed for authentication and encryption (the latter, if using ESP protocol) to pre-compensate for the effect of the NAT translations on the cryptographic or non-

cryptographic checksums. Thus, when the packet is received at its destination and authenticated and decrypted (the latter, if using ESP protocol), the checksum calculated for that packet will be in accord with the transmitted checksum that was incorporated into and transmitted in the packet. Thus, absent a transmission error, the packet will not be dropped by the receiver. Specifically, before the packet is authenticated and encrypted (the latter, if using ESP protocol), private IP addresses and port numbers that NAT will not translate are replaced by corresponding assigned global values; the TCP or UDP checksum is modified to account for all the translations in the packet from private IP addresses and port numbers to global IP addresses and port numbers in such a manner that when NAT performs its translation operations and the packet is sent to its destination, the modified checksum matches, absent a transmission error, the actual checksum of the packet as operated on by NAT; and the AH authentication data (for AH protocol) is computed as if the source IP address were equal to the global IP address. For an incoming packet from the network, in a similar manner, the AH authentication data (for AH protocol) is computed as if the destination IP address were equal to the global IP address. After the packet is then authenticated and decrypted (the latter, if using ESP protocol) by the client, it is modified so as to post-compensate for the effect of the NAT translations on the cryptographic or non-cryptographic checksums. Specifically, the client replaces those global IP addresses and port numbers in the packet that NAT has not translated with their corresponding private values . Further, the TCP or UDP checksum is modified to compensate for the translations made by the client and the NAT to the IP addresses and port numbers so that the modified checksum matches, absent a transmission error, the checksum calculated over the address-translated packet.